IT-Security Monitoring

Risiken objektiv bewerten

Ohne Investitionen in eigene Security-Monitoring-Lösungen können Sicherheitsverantwortliche einen objektiven Überblick der IT-Sicherheitslage in ihrem Unternehmen erhalten.

In keinem anderen Bereich der IT wird so viel Geld für präventive Maßnahmen ausgegeben, wie im Bereich IT-Security. Und diese Investitionen erfolgen meist ohne konkreten Nachweis des tatsächlichen Nutzens. Das liegt zum einen daran, dass die Wirksamkeit von IT-Security nur schwer zu überprüfen ist, da sie sich nicht nur gegen bereits bekannte Angriffsmuster richtet, sondern auch neue und bisher unbekannte Attacken erkennen und verhindern soll. Zum anderen fehlen häufig Informationen zum tatsächlichen Sicherheitsstatus und zu Schwachstellen – oder diese Informationen werden aus Mangel an Ressourcen und Fachkenntnissen nicht ausreichend beachtet und ausgewertet.

Ansatzpunkt für IT-Security Monitoring in Form von Managed Services. Der wesentliche Unterschied zu klassischen Tools und Werkzeugen besteht darin, dass ein Security Operation Center (SOC) zum Einsatz kommt,

das die Security-Vorfälle bewertet, klassifiziert sowie priorisiert und damit den Betriebsaufwand für den Kunden erheblich reduziert.

Um Security Monitoring wirklich effizient durchzuführen, ist es notwendig, möglichst viele Informationsquellen zu nutzen. Hierbei handelt es sich beispielsweise um Schwachstellen in Applikationen oder Betriebssystemen, Änderungen im Kommunikationsverhalten, protokollfremde Datenübertragungen, Konfigurationsänderungen und Fehlermeldungen, aber auch Angriffsmeldungen von bereits vorhandenen Security-Systemen wie Firewalls, IDS-Systemen oder Virenscannern.

Zur Sammlung dieser Informationen kommen hauptsächlich drei Technologien zum Einsatz. An erster Stelle steht sicherlich die Schwachstellenerkennung (Vulnerability Management), die eine aktuelle Übersicht der bekannten Schwachstellen liefert und damit als Basis für eine spätere Priorisierung der Risiken dient. Eine weitere Maßnahme ist das Security Incident & Event Management (SIEM), das durch Auswertung von Log-Daten zusätzliche Hinweise auf kritische Vorgänge bereitstellt. Darüber hinaus sollte eine Analyse des Netzwerkdatenverkehrs – Network Intrusion Detection (NIDS) – erfolgen, um sowohl Signatur-basiert als auch Verhaltens-basiert kritische Aktivitäten wie Malware, Anomalien und andere Risiken im Netzwerkverkehr unmittelbar zu erkennen.

Auf Basis dieser Informationsquellen kann eine sinnvolle Korrelation erfolgen. Dabei wird zum Beispiel eine Verbindung zwischen erkannten Angriffen und vorhandenen Schwachstellen hergestellt, wodurch eine korrekte Priorisierung möglich ist.

Jedoch liefern selbst die besten Korrelationsmechanismen immer noch Security Events in einer Größenordnung, die für den Endkunden in der Praxis kaum zu bewältigen sind. Zudem stellt das Aussortieren von Fehlalarmen (False Positives) für den Anwender eine weitere, nicht leicht zu bewältigende Hürde dar, verfügt er doch in den seltensten Fällen über qualifiziertes Fachpersonal. Deshalb ist die abschließende Bewertung durch das SOC ein wesentlicher Mehrwert von Managed Services und gleichzeitig die Voraussetzung für die Bereitstellung von geprüften Security Incidents, die unmittelbar durch die jeweilige Fachabteilung oder den verantwortlichen Dienstleister bearbeitet werden können.

Darüber hinaus kann bei schwerwiegenden Sicherheitsvorfällen eine qualifizierte Alarmierung über das SOC erfolgen. Der Kunde kann die Sicherheitsvorfälle somit unmittelbar bearbeiten – ohne eine nochmalige zeitintensive Prüfung.

Risikowert und Risk Dashboard. In der Praxis hat sich gezeigt, dass sich mit einem zielgruppenorientierten Reporting die Akzeptanz der IT-Security im Unternehmen erheblich steigern lässt. Als besonders geeignet hat sich dabei die Darstellung eines unternehmensweiten Risikowertes erwiesen, der die tatsächliche Risikolage genauso berücksichtigt wie die Bearbeitungsgeschwindigkeit und die Lösungsrate. Dieser Risikowert schafft Transparenz über alle Unternehmensbereiche hinweg – einschließlich der Geschäftsführungsebene – und bietet eine geeignete Grundlage für Diskussionen auch auf nicht-technischer Ebene. Strategische Entscheidungen lassen sich fundiert untermauern und Budgetdiskussionen erheblich erleichtern, da die vorgeschlagenen Maßnahmen eindeutig belegbar sind.

Ein Risk Dashboard bietet ergänzend die Möglichkeit, den Risikostatus der Systeme, der IT-Prozesse und gegebenenfalls der Business-Prozesse grafisch darzustellen – analog zur Darstellung der System- oder Serviceverfügbarkeit, die aus dem Infrastruktur- und Service-Monitoring hinlänglich bekannt ist. Damit ist es auf einen Blick möglich, sich einen Überblick über die aktuelle Risikosituation zu verschaffen. In Kombination mit der Verfügbarkeitsdarstellung ergibt sich also ein vollständiger Betriebsstatus der Unternehmens-IT.

» **Um Security Monitoring wirklich effizient durchzuführen,** ist es notwendig, möglichst viele Informationsquellen zu nutzen. «

Fazit. Zusammenfassend kann gesagt werden, dass sich durch IT-Security Monitoring als Managed Services im Wesentlichen die folgenden drei Ziele erreichen lassen:

Erstens gewinnt der Kunde jederzeit einen aktuellen und vor allem objektiven Überblick über die IT-Sicherheitslage seines Unternehmens. Zweitens können aufgrund dieses Überblicks Investitionen zielgerichtet erfolgen und Schwachstellen effizient geschlossen werden. Und drittens fallen für den Kunden weder Investitionen noch Betriebsaufwand für die Security-Monitoring-Lösung selbst an. Folglich müssen auch keine Ressourcen vorgehalten werden. Das vorhandene Personal kann sich einerseits auf die Bearbeitung der Incidents konzentrieren und andererseits das Kerngeschäft des Unternehmens besser unterstützen.

Jedes Unternehmen steht heute vor der Frage, wie es mit IT Security- und Cyber-Risiken umgehen soll. IT-Security Monitoring schafft die Grundlage für einen angemessenen Umgang mit diesen Risiken, ohne die wirtschaftlichen Aspekte außer Acht zu lassen.

Christian Bohr

Christian Bohr,
Head of Managed Services,
Controlware GmbH,
www.controlware.de